UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, Plaintiff, v. NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a sipretail.com, Defendants.	Civil Action No. 20-CV-473 (EK) (RLM)

DECLARATION OF DAVID FRANKEL

I, David Frankel, have personal knowledge of the facts set forth below, and if called as a witness I would testify as follows:

1. I am a citizen of the United States and I reside in Monte Sereno, California. I own and operate ZipDX LLC, a company I founded in 2007 to deliver novel remote collaboration services via the telephone and Internet. ZipDX makes use of domestic and international voice services, but is not itself a voice-over-internet-protocol ("VoIP") carrier. I am intimately familiar with many technical and business aspects of the industry.

2. I have worked in the computer hardware and software fields since 1974, including work on supercomputer and high-performance networking and in telecommunications. I hold a Bachelor of Science degree in Electrical Engineering from the University of Illinois at Urbana-Champaign. I hold ten U.S. patents in the field of telecommunications. I am familiar with a variety of telephony protocols including SS7, ISDN, SIP, SHAKEN and STIR, and I am listed as a contributor to STIR RFC 8224.

3. In drafting this declaration, I reviewed the declarations of John Dalrymple, Dean Hansen, Nicholas Palumbo, Natasha Palumbo, the declaration of Special Agent Clayton Gerber dated February 25, 2020, the declaration of Special Agent Marcy Ralston dated January 28, 2020, and the Complaint in this matter.

USTELECOM INDUSTRY TRACEBACK GROUP AND TRACEBACKS OF FRAUDULENT CALLS

4. I became involved in illegal robocall mitigation in 2013. Since that time, I have spoken at numerous industry events, submitted filings and participated in meetings with the United States Federal Communications Commission. On June 17, 2019, I testified regarding illegal robocalls before the U.S. Senate Special Committee on Aging.

5. My company has a part-time contract supporting USTelecom's Industry Traceback Group ("ITG"). USTelecom is a nonprofit trade association for the U.S. broadband and communications industry. USTelecom has developed the ITG across the telecommunications industry to trace robocalls to their sources. I work as a consultant to the ITG and I manage the portal that completes call tracebacks.

6. A traceback is the process of determining the origin of a telephone call. A telephone call may go through several hops, meaning that the call may transit through several different intermediary service providers, as it proceeds from the source (call originator) to the destination (the call termination point, in this context a U.S.-based consumer). Within the United States, telecommunications companies facilitate tracebacks, allowing the ITG to start with the destination and trace the call back through various providers to identify the source of a call, or – for calls originating overseas – the point at which the call entered the United States.

7. There are approximately five billion robocalls placed monthly. The telecommunications industry is aware that a large fraction of those calls involve fraudulent campaigns. Further, a relatively small number of perpetrators are responsible for a large fraction of the problem. By tracing back a handful of calls from any given campaign, the ITG is able to find the source of the campaign.

8. No telephone call can reach a United States telephone number without going through some U.S.-based telecommunications provider that places that call onto the U.S. telecommunications network, almost always in exchange for a payment from the source of the call or an intermediary.

INVESTIGATION INTO SOCIAL SECURITY ADMINISTRATION IMPOSTER FRAUD CAMPAIGNS IN JUNE 2019

9. In my work with USTelecom, we identified Social Security Administration ("SSA") impersonation calls as a particularly egregious campaign, due to the number of people victimized and the amount of money victims were losing. Through the USTelecom on-line system, the ITG initiated tracebacks of five SSA impersonation calls. The first led back to Ecommerce, d/b/a TollFreeDeals ("TollFreeDeals"). TollFreeDeals responded promptly to the automated traceback message, but given the severity of this campaign, I spoke to Mr. Palumbo by phone and then followed up with an email.

10. During our telephone conversation on June 3, 2019, Mr. Palumbo identified [redacted], as the specific customer in India that had sent the call. When we spoke, Mr. Palumbo stated that on that day he had processed about five million calls from this customer and the USTelecom traceback notification was the first complaint he had received about this customer. I told him that I was not surprised he had not received a complaint earlier because until we had completed the traceback, we did not know who was transmitting the fraudulent SSA

calls, and thus, no one would know to direct a complaint to TollFreeDeals. I explained the point of our traceback effort was to highlight the calls so that action could be taken.

11. On that same call, I provided Mr. Palumbo with details of the other four SSA fraud call tracebacks we had in process and he verified that these calls all came from [redacted] the same customer in India. Mr. Palumbo and I continued to correspond via email concerning the SSA fraud calls. *See* email chain, dated June 3, 2019, attached hereto as Exhibit 1.

12. Mr. Palumbo provided me with an email address for [redacted]. On June 3, 2019, I emailed [redacted] at the address Mr. Palumbo supplied and copied Mr. Palumbo on that message. *See* email chain, dated June 3-June 6, 2019, attached hereto as Exhibit B. In my email to [redacted] and Mr. Palumbo, I wrote: "[G]oing forward, we would ask that you take steps to prevent your clients (existing and new) from making illegal calls to USA . . . . In particular, you should not permit customers to have access to high-volume calling capability, and to use any calling number of their choosing (and especially +1 telephone numbers). Only under special circumstances would a legitimate caller need this. If you do grant access to high-volume calling, please make sure you have a valid business name and registration, physical address, a web site for the business, and names of executives with professional email addresses along with telephone numbers. Also record the justification for high-volume calling (and caller-ID spoofing if you grant that capability). This will be important if problems do arise. It will also be important for you to monitor your customers' traffic to make sure they stay in compliance." Within the email, I included a link to a white paper that explains the robocalling landscape and includes steps to take to mitigate illegal calls including: examining all traffic from that customer; imposing

network-level constraints; restricting the number of concurrent calls; and limiting the caller-ID value(s) available for the customer's use. [redacted] never responded to my email.

13. I implored Mr. Palumbo to take swift action to stop the calls, and he assured me he was working with his customer. *See* Exhibit 2. Over the next two days, we exchanged additional emails. *Id.*

14. On June 5, 2019, Mr. Palumbo emailed that he was waiting for confirmation, but "it look[ed] like action was taken" by [redacted] *Id.* On the same day, I responded that we were still seeing a huge number of calls and I provided him with call examples. *Id.* I emailed him: "I'm running out of patience. We need ZERO of these calls coming in. There's no excuse for it. Your customer in India should not be sending ANY calls from +1 numbers unless they've explained to you why they would need to do that. I can't tell you what to do and I don't like making threats. These calls are very serious violations of federal laws and it shouldn't take multiple days to turn it off. 'Waiting for confirmation' isn't something this illegal operator deserves and could, I would think, get you in trouble. I'm happy to connect on the phone if you want to brainstorm how to be more proactive and effective on this. Here are 7 more calls, none of which should have happened. These are just examples; the calls are flooding in as you should be able to readily observe from your own records." I listed details for seven SSA fraud calls we captured that day.

15. Mr. Palumbo responded a few hours later: "I reemed [*sic*] my client out today. I think it stopped. Please let me know if you see anything else." *Id.* I emailed back that, rather than waiting to see what happened, there were actions he could take; I included specific mitigating actions including: "[s]ee how many calls they are sending per minute, and what their average call duration is, and whether they are using +1 phone numbers for their caller-ID. If they are sending thousands of calls, and their average call duration is less than a minute, we know

these are unwanted calls. And if they are using many different +1 phone numbers for caller-ID, then they are illegally spoofing. I would appreciate it if you could share your findings." Mr. Palumbo did not respond.

16. The next day, June 6, 2019, I emailed Mr. Palumbo and included five examples of new SSA fraud calls from that morning. *Id*. He did not respond to that email.

17. Mr. Palumbo continued to receive notices from our automated system as the calls continued. At the end of June, he informed us he would not respond to our traceback requests, but would only respond to subpoenas. In August 2019, he did respond to US Telecom traceback requests, indicating again [redacted] as the source of the calls. Subsequently he identified other India-based sources as well. Aside from identifying the source of the calls, Mr. Palumbo did not take any of the other mitigation steps outlined in my emails to him.

INDICATORS OF FRAUDULENT ROBOCALLS

18. The ability to place many calls rapidly (high calls-per-second, or CPS), and the ability to sustain many simultaneous calls (sessions), while sometimes used legitimately, are very often abused. Few legitimate callers need the ability to place millions of calls daily. When one customer has huge call volumes, and a high percentage of those calls are unanswered or are of short duration, those indicators – particularly combined – raise a red flag and point to fraudulent call traffic.

19. Similarly, one customer using millions of different caller-ID values is also an indicator of fraudulent call traffic. Few, if any, entities have a legitimate need to use millions of different caller-ID values. Certainly, school districts and entities sending calls about

prescriptions would not have a need for such a large group of numbers.[1] Such characteristics are not exclusive to fraudulent calls, but they are indicative of the likelihood of such calls, which rises with the scale of those call characteristics. Most providers do not, by default, enable their customers to access these capabilities – e.g., huge call volumes, ability to place hundreds of calls per second, the use of large numbers of caller-ID values – unless the provider has good knowledge of the customer and understands the planned use of those capabilities.

20. When the indicators above are combined with definitive information that at least some of the call traffic consists of illegal and fraudulent calls, a prudent telecommunications provider would engage with its customer to mitigate the fraud and take necessary steps to restrict the calls. A telecommunications provider would solicit additional explanations from the customer (proceeding upstream in the call path as necessary). If satisfactory explanations were not rapidly forthcoming, and if other steps taken to restrict the calls were not effective, then the effective remedy would be to discontinue all traffic from the offending customer. Every day – every hour – that passes without effective mitigation means that fraudulent, illegal activity continues unchecked.

21. Investigation and follow-up with customers to prevent fraudulent robocalls require energy and effort. Fraud is almost as old as the telephone itself (reference Almon Brown Strowger, who in 1889 invented an early telephone switching system to prevent human operators from purposefully and mischievously redirecting telephone calls). Attention to fraud prevention

[1] For example, if a call center were calling on behalf of Walgreens, perhaps they would use as source numbers the telephone numbers of Walgreens' stores – there are almost 10,000 of them. But there is no legitimate business purpose for extremely large groups of different caller ID values. Even a need for 10,000 unique source numbers is so rare that telecommunications providers generally require a justification for this request.

is part of being a responsible provider. Providers that lack means to keep problematic traffic off their network must not offer services that attract illegal robocallers.

22. Of the thousands of VoIP providers in the United States, the vast majority are not conduits of significant ongoing illegal robocalling. Many providers have terms of service and acceptable use policies that prohibit illegal calling and use economic penalties to dis-incentivize short duration calling; they also use tools to monitor for suspect calling patterns. In contrast, defendants have been dismissive in their response to complaints of fraudulent robocalls, thus perpetuating the problem.

Pursuant to 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Dated: February 29, 2020
Monte Sereno, California.

David Frankel